VERSION WITH MARKINGS TO SHOW CHANGES MADE

IN THE ABSTRACT OF THE DISCLOSURE

The Abstract of the Disclosure has been amended as follows:

--[The present invention relates to a] A transmission apparatus, a reception apparatus, a transmission method, and a reception method, which are used for transmission and reception of encrypted digital data protected against illegal decryption of the encrypted digital data by a third party capable of inferring an encryption algorithm by decryption of a pattern having a known pre-encryption value, and [relates to] a recording medium for recording the encrypted digital data.--

IN THE CLAIMS

Claims 2-12 and 14-41 have been amended as follows:

--2. (Amended) [A] The transmission apparatus according to claim 1, wherein said transmission means transmits said encrypted digital data [to other equipment] by radio or wire communication.

--3. (Amended) [A] The transmission apparatus according to claim 1, wherein said transmission means transmits said encrypted digital data as data to be recorded onto a recording medium.

--4. (Amended) [A] The transmission apparatus according to claim 1, wherein said insertion means inserts said random data into an invalid-data portion existing in said packet.

--5. (Amended) [A] The transmission apparatus according to claim 1, wherein [the] a length of an encryption unit encrypted by said encryption means is smaller than [the] a length of said packet-converted digital data.

--6. (Amended) [A] The transmission apparatus according to claim 5, wherein said insertion means inserts said random data into said encryption unit.

--7. (Amended) A reception apparatus for receiving encrypted digital data that has been converted into packets, including random data [in each packet] within said packets of said encrypted digital data, said reception apparatus comprising:

reception means for receiving said encrypted packet-converted digital data;

decryption means for decrypting said encrypted packet-converted digital data received by said reception means; and

elimination means for removing said random data from said packet-converted digital data obtained as a result of decryption carried out by said decryption means.

--8. (Amended) [A] The reception apparatus according to claim 7, wherein said reception means receives said encrypted digital data [from other equipment] by radio or wire communication.

--9. (Amended) [A] The reception apparatus according to claim 7, wherein said reception means receives said encrypted digital data recorded on a recording medium.

--10. (Amended) [A] The reception apparatus according to claim 7, wherein said elimination means [eliminates] removes said random data by removing an invalid-data portion existing [in] within said [packet] packets.

--11. (Amended) [A] The reception apparatus according to claim 7, wherein [the] a length of a decryption unit decrypted by said decryption means is smaller than [the] a length of said packet-converted digital data.

--12. (Amended) [A] The reception apparatus according to claim 11, wherein said elimination means [eliminates] removes said random data from said decryption unit.

--14. (Amended) [A] The transmission method according to claim 13, wherein [the] a length of an encryption unit to be encrypted is smaller than [the] a length of said packet-converted digital data and said random data is inserted

into said encryption unit.

--15. (Amended) A reception method for receiving encrypted digital data that has been converted into packets including random data [in each packet] within packets of said encrypted digital data, said reception method comprising the steps of:

receiving encrypted packet-converted digital data;

decrypting said received encrypted packet-converted digital data; and

removing random data from said packet-converted digital data obtained as a result of decrypting said received encrypted packet-converted digital data.

--16. (Amended) [A] The reception method according to claim 15, wherein [the] a length of a decryption unit to be decrypted is smaller than [the] a length of said packet-converted digital data and said random data [is] removed from said decryption unit.

--17. (Amended) A transmission apparatus for encrypting a program comprising a continuous data stream and transmitting said encrypted program, said transmission apparatus comprising:

random-data-generating means for generating random data;

addition means for adding said random data generated by said random-data-generating means to [the] a beginning and

[the] an end of said program;

encryption-processing means for encrypting said program including said random data added thereto by said addition means; and

transmission means for transmitting said program encrypted by said encryption-processing means.

--18. (Amended) [A] The transmission apparatus according to claim 17, wherein said transmission means transmits said encrypted digital data [to other equipment] by radio or wire communication.

--19. (Amended) [A] The transmission apparatus according to claim 17, wherein said transmission means transmits said encrypted digital data as data to be recorded onto a recording medium.

--20. (Amended) [A] The transmission apparatus according to claim 17, wherein [the] a data length of said random data generated by said random-data-generating means is variable.

--21. (Amended) A reception apparatus for receiving an encrypted program comprising a continuous data stream, said reception apparatus comprising:

reception means for receiving said encrypted program comprising [a] said continuous data stream;

decryption means for decrypting said encrypted program

comprising [a] said continuous data stream received by said reception means; and

elimination means for removing random data from [the] a beginning and [the] an end of a program obtained as a result of said decryption carried out by said decryption means.

--22. (Amended) [A] The reception apparatus according to claim 21, wherein said reception means receives said encrypted digital data [from other equipment] by radio or wire communication.

--23. (Amended) [A] The reception apparatus according to claim 21, wherein said reception means receives said encrypted digital data recorded on a recording medium.

--24. (Amended) [A] The reception apparatus according to claim 21, wherein [the] a data length of said random data removed by said elimination means is variable.

--25. (Amended) A transmission method for encrypting a program comprising a continuous data stream and transmitting said encrypted program, said transmission method comprising the steps of:

generating random data;

adding said generated random data to [the] a beginning and [the] an end of said program;

encrypting said program including said added random data;

and

transmitting said encrypted program.

--26. (Amended) A reception method for receiving an encrypted program comprising a continuous data stream, said reception method comprising the steps of:

receiving said encrypted program comprising [a] said continuous data stream;

decrypting said received encrypted program comprising [a] said continuous data stream; and

removing random data from [the] a beginning and [the] an end of a program obtained as a result of decrypting said received encrypted program.

--27. (Amended) A transmission apparatus for encrypting a plurality of data blocks comprising main data and additional data and transmitting said encrypted data blocks, said transmission apparatus comprising:

additional-data-inserting means for carrying out processing to insert additional data into data blocks randomly selected [at random] from among a sequence of said data blocks composing a stream of said main data;

encryption means for encrypting said sequence of data blocks after said processing carried out by said additional-data-inserting means to insert said additional data; and

transmission means for transmitting said sequence of data

blocks encrypted by said encryption means.

--28. (Amended) [A] The transmission apparatus according to claim 27 [wherein], further comprising:

[there is further provided] random-data-inserting means for carrying out processing to insert random data into [some] selected ones of said data blocks[; and], wherein

said encryption means encrypts said sequence of data blocks after said processing carried out by said additional-data-inserting means to insert said additional data and said processing carried out by said random-data-inserting means to insert said random data.

--29. (Amended) [A] The transmission apparatus according to claim 27, wherein said additional data inserted by said additional-data-inserting means into said data blocks selected at random is unencrypted data.

--30. (Amended) [A] The transmission apparatus according to claim 27, wherein said additional data inserted by said additional-data-inserting means into said data blocks selected at random is unencrypted data and encrypted data.

--31. (Amended) [A] The transmission apparatus according to claim 28, wherein said random-data-inserting means inserts random data into an invalid-data portion [in] within each [of some] said selected ones of said data blocks.

--32. (Amended) [A] The transmission apparatus according to claim 27, wherein said transmission means transmits said sequence of data blocks [to other equipment] by radio or wire communication.

--33. (Amended) [A] The transmission apparatus according to claim 27, wherein said transmission means transmits said sequence of data blocks as data to be recorded onto a recording medium.

--34. (Amended) A transmission method for encrypting a plurality of data blocks comprising main data and additional data and transmitting said encrypted data blocks, said transmission method comprising the steps of:

carrying out processing to insert additional data into data blocks randomly selected [at random] from among a sequence of said data blocks composing a stream of said main data;

encrypting said sequence of data blocks after said processing to insert additional data; and

transmitting said sequence of encrypted data blocks.

--35. (Amended) [A] The transmission method according to claim 34, said transmission method further [including] comprising the step of [carrying out] processing to insert random data into [some] selected ones of said data blocks, [whereby] wherein said sequence of data blocks is encrypted

after said step of [carrying out] processing to insert said additional data and said step of [carrying out] processing to insert said random data.

--36. (Amended) A recording medium for recording at least an encrypted program, wherein[,] before being recorded [into] onto said recording medium, said program is encrypted after random data is added to [the] a beginning and/or [the] an end of said program.

--37. (Amended) A recording medium for recording packet-converted and [then] encrypted digital data, wherein[,] before being recorded into said recording medium, said packet-converted data is encrypted after random data is added to part of said packet-converted data.

--38. (Amended) A recording medium for recording a plurality of encrypted data blocks comprising main data and additional data, wherein[,] before being recorded into said recording medium, said plurality of encrypted data blocks are obtained by inserting additional data into selected ones of said data blocks randomly selected [at random] from among a sequence of said data blocks composing a stream of said main data and by encrypting said data blocks selected from said sequence of said data blocks including said additional data.

--39. (Amended) [A] The recording medium according to

claim 38, wherein[,] after said additional data is added, random data is inserted into some of said data blocks of said sequence of said data blocks before encrypting said data blocks selected from said sequence of data blocks including said random data.

--40. (Amended) [A] The recording medium according to claim 38, wherein said additional data inserted into said data blocks selected at random is unencrypted data.

--41. (Amended) [A] The recording medium according to claim 38, wherein said additional data inserted into data blocks selected at random is encrypted data and unencrypted data.--